UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/879,575	06/12/2001	James Alexander Reeds III	1999-0275/037-0039	4755

52218 7590 07/20/2009

AT&T Legal Department - ZO
Attn: Patent Docketing
Room 2A-207
One AT&T Way
Bedminster, NJ 07921

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2433	

MAIL DATE	DELIVERY MODE
07/20/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/879,575	REEDS ET AL.	
	Examiner	Art Unit	
	ELLEN TRAN	2433	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 March 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-16,18-22,26-32,41-43,45-47 and 57* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3, 5-16, 18-22, 26-32, 41-43, 45-47, and 57* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application.
6) ☐ Other: _____.

Detailed Action

1. This action is responsive to communication filed on: 30 March 2009 with acknowledgement of an original application filed on 12 June 2001.

2. Claims 1-3, 5-16, 18-22, 26-32, 41-43, 45-47, and 57, are currently pending in this application. Claims 1, 14, 41, and 57 are independent claims.

Response to Arguments

3. Applicant's arguments filed 30 March 2009 have been fully considered however they are not persuasive.

I) In response to Applicant's argument beginning on page 2 with respect to claims 1, 14, and 41, as well as their dependent claims, *"Nowhere does Medvinsky, teach or suggest padding data to generate padded data, applying the fixed length segment to the data to form an encrypted payload and applying a remaining portion of the fixed length segment to the padding, de-padding the padded encrypted data to form the encrypted payload, and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet as required by the independent claims".*

The Examiner disagrees with argument. It is the Medvinsky and Jung combination that teaches the padding and encrypted payload, see Jung paragraph 35. Jung teaches that during the encryption decryption process padding is applied where applicable. The phrase 'where applicable' implies that as is known in the art null data is applied to maintain the length of the payload or key segment for encryption. Padding is well known in the art and is suggest by both references. Medvinsky teaches in paragraph 57 that the size of the random key stream pad changes causing to rekey and start a new RC4, therefore the combination of Medvinsky and Jung

suggests that padding can be used for encryption and decryption. Padding is a well known concept in addition the applicant's own disclosure paragraph 26 indicates "the encryption engine 306 uses RC4 cipher stream encryption techniques to apply a forward ciper key 308 to the padded data to produce the encrypted padded payload". Therefore it is obvious that the padding suggested by the combination of Medvinsky and Jung is equivalent to the claimed padded data, note both the applicant's disclosure and Medvinsky teach padding with respect to RTP and RC4 encryption.

II) In response to applicant's argument beginning on page 3 with respect to claims 1, 14, and 41, as well as their dependent claims, *"Jung fails to compensate for the shortcoming of Medvinsky. Jung teaches that [t] encryption/decryption module 24 is primarily ... Padding data where applicable, as taught by Jung fails to teach or suggest padding data to generate padded data, applying the fixed length segment to the padded data to form padded encrypted data by applying a portion of the fixed length segment to the data to form an encrypted payload and applying a remaining portion of the fixed length segment to the padding, de-padding the padded encrypted data to form the encrypted ...".*

The Examiner disagrees with argument. The following is noted, the applicant's invention is directed to an apparatus, system and method to maintain synchronization of an encryption key stream at the transmitter to a decryption key stream at a receiver [See Applicant's Abstract]. It is noted 'fixed segment of the continuous encryption key stream' that is selected is dependent upon the session count. The Examiner interprets this type of 'encryption key stream' encryption method equivalent to the well known streaming encryption method that maintains synchronization by the Real Time Protocol (RTP). This type of streaming encryption is used for

communicating voice packets over the Internet. The following references are noted all of which discuss sending voice of IP (VOIP) with the use of RTP synchronization as well as padding.

Kikuchi et al. U.S. Patent 7,010,032 col. 5, lines 43-56

Mohaban et al. U.S. Patent 7,002,993 col. 6, lines 21-48

Maes U.S. Patent 6,970,935 col. 18, lines 24-47

Lahat U.S. Patent 6,963,561 col. 17, lines 52-64

Tomita U.S. Patent 6,947,448 col. 1, lines 53-64

Mahler U.S. Patent 6,542,504 col. 8, lines 15-20

Therefore the Examiner asserts the applicant's claims of padding with RTP encryption is well known in the art.

III) In response to applicant's argument beginning on page 4 with respect to claims 1, 14, and 41, as well as their dependent claims, *"If the claim extends to what is obvious, it is invalid under § 103." See id. To be nonobvious, an improvement must be "more than a predictable use of prior art elements according to their established function ... Both padding data and de-padding padded, encrypted data to form the encrypted payload, as required by claim 14 is not a predictable result of the requirement of stream encryption algorithms that the transmitter and receiver sides by synchronized".*

The Examiner disagrees with argument. As shown above RTP encryption mechanisms utilize padding. The 'de-padding' is an understood variation just as encryption and decryption. Therefore the padding and de-padding of the stream encrypted with a RTP protocol utilizes padding and de-padding. In addition both references Medvinsky and Jung are directed to streaming encryption.

IV) In response to applicant's argument beginning on page 14 with respect to claim 57, *"Medvinsky, alone or in combination with Sengodan, fails to teach or suggest a receiver including a padding engine ... Sengodan fails to compensate for the shortcoming of Medvinsky"*

The Examiner disagrees with argument. As noted above Medvinsky does suggest padding in addition the combination teaches the feature see Sengodan col. 4, lines 30-36.

V) In response to applicant's argument beginning on page 16 with respect to claim 57, *"The receiver of Sengodan that receives the encrypted padded data and an indicator of the amount of padding teaches away from a receiver including a padding engine operable to pad an encrypted payload of the received encrypted data packet to generate the padded encrypted payload of the received encrypted data received by the decryption engine"*

The Examiner disagrees with argument. The entire references must be reviewed for all they teach or suggest. Both references are directed to streaming encryption mechanisms that utilize RTP protocols to synchronize the received and transmitted encrypted and decrypted payload. Padding and de-padding are mechanisms that are suggested and well known. See Medvinsky paragraph 57 as well as Sengodan [Abstract].

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1-3, 5-8, 14-16, 18-22, 26, 27, 41-43, and 45-47** are rejected under 35 U.S.C. 103(a) as being unpatentable over Medvinsky U.S. Patent Application Publication No. 2002/0094081 (hereinafter '081) in view of Jung U.S. Patent Application Publication No. 2001/0052072 (hereinafter '072).

As to independent claim 1, "A method comprising: selecting a fixed length segment of a continuous decryption key stream based on a received session count of a received data packet" is taught in '081 pages 3-4 paragraphs 0033-0034;

the following is not explicitly taught in '081:

"padding an encrypted payload of the received data packet to a given size with padding, the given size corresponding to the fixed length segment size, and decrypting the payload of the received data packet by applying a portion of the fixed length segment to the received data packet by applying the fixed length segment of the continuous decryption key to the padded, encrypted payload, a portion of the fixed length segment being applied to the encrypted payload, a remaining portion of the fixed length segment being applied to the padding" however '072 teaches that padding is done by the encryption/decryption module as needed to perform the encryption/decryption operations on page 3, paragraph 0035. Applying padding would be applicable in the decryption and encryption process. Also note the RTP protocol implements padding when specified in transmission.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method encryption/decryption utilizing stream ciphers over the Internet taught in '081 to include a means to incorporate the padding into the encryption and decryption module. One of ordinary skill in the art would have been motivated to perform such a modification because there

is a requirement of stream encryption algorithms is that the transmitting side and the receiving side be synchronized see '072 (pages 1, paragraphs 0013). "A requirement of stream encryption algorithms is that the transmitting side and the receiving side be synchronized in order for the encryption and decryption to work properly. Specifically, the data must be decrypted in the same order or sequence in which it was encrypted. However, such synchronization is not only difficult to employ and maintain in the IP network 10, but can also consume a significant amount of bandwidth (e.g., 7-10% using RTP)".

As to dependent claim 2, "wherein the applying comprises performing a bit per bit streaming encryption process" is disclosed in '081 page 3, paragraph 0034.

As to dependent claim 3, "wherein the applying further comprises performing an exclusive OR operation with the portion of the fixed length segment and the data packet" is taught in '081 page 3, paragraph 0034.

As to dependent claim 4, "wherein the applying further comprises performing an RC4 operation with the portion of the fixed length segment and the data packet" is shown in '081 page 3, paragraph 0034.

As to dependent claim 5, "further comprising: receiving the data packet, the data packet comprising at least a portion of the received session count" is shown in '081 page 2, paragraphs 0017-0018.

As to dependent claim 6, "wherein the data packet further comprise at least a portion of a received message digest value" is disclosed in '081 page 4, paragraph 0054.

As to dependent claim 7 "wherein the selecting comprises: selecting a current fixed length segment if a difference between the received session count and a locally generated session count is less than a threshold value" is shown in '081 page 4, paragraphs 0036-0051.

As to dependent claim 8, "wherein the selecting further comprises: extracting the at least a portion of the received session count from the encrypted data packet; expanding the at least a portion of the received session count to the received session count; and comparing the received session count to the locally generated session count" is disclosed in '081 pages 3-4 paragraphs 0033-0034.

As to independent claim 14, "A method of generating an encrypted data packet, the method comprising: selecting a fixed length segment of a continuous encryption key stream" is taught in '081 pages 3-4 paragraphs 0033-0034;

"generating a session count based in accordance with the fixed length segment; and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet" is shown in '081 page 2, paragraphs 0017-0018;
the following is not explicitly taught in '081:

"padding data to generate padded data" and **"applying the fixed length segment to the padded data to form padded encrypted data by applying a portion of the fix length segment to the data to form an encrypted payload and applying a remaining portion of the fixed length segment to the padding; de-padding the padded encrypted data to form the encrypted payload"** however '072 teaches that padding is done by the encryption/decryption module as needed to perform the encryption/decryption operations on page 3, paragraph 0035.

Applying padding would be applicable in the decryption and encryption process. Also note the RTP protocol implements padding when specified in transmission.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method encryption/decryption utilizing stream ciphers over the Internet taught in '081 to include a means to incorporate the padding into the encryption and decryption module. One of ordinary skill in the art would have been motivated to perform such a modification because there is a requirement of stream encryption algorithms is that the transmitting side and the receiving side be synchronized see '072 (pages 1, paragraphs 0013). "A requirement of stream encryption algorithms is that the transmitting side and the receiving side be synchronized in order for the encryption and decryption to work properly. Specifically, the data must be decrypted in the same order or sequence in which it was encrypted. However, such synchronization is not only difficult to employ and maintain in the IP network 10, but can also consume a significant amount of bandwidth (e.g., 7-10% using RTP)".

As to dependent claims 15 and 16, these claims contain substantially similar subject matter as claims 2 and 3; therefore they are rejected along the same rationale.

As to dependent claim 18, "further comprising: generating a message digest value; and combining at least a portion of the message digest value with the encrypted payload to form the encrypted data packet" is taught in '081 page 4, paragraphs 0054 –0055.

As to dependent claim 19, "wherein the generating comprises: generating the message digest value based on the encrypted payload, the session count and a message digest key" is shown in '081 page 4, paragraphs 0054 –0055.

As to dependent claim 20, "further comprising: forming the at least a portion of the message digest value by truncating the message digest value" is disclosed in '081 page 4, paragraphs 0054 –0055.

As to dependent claim 21, "further comprising transmitting the encrypted data packet to a receiver through a communication channel" is taught in '081 page 2, paragraph 0016.

As to dependent claim 22, "further comprising: receiving a received data packet corresponding to the encrypted data packet, the received data packet comprising the encrypted payload, at least a portion of a received session count and a received truncated message digest value; selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet; and decrypting a payload of the data packet by applying a portion of the fixed length segment to the data packet" is shown in '081 pages 3-4 paragraphs 0033-0034 and page 4, paragraphs 0053-0055.

As to dependent claims 26 and 27, these claims contain substantially similar subject matter as claims 2-8; therefore they are rejected along the same rationale.

As to independent claim 41, this claim is directed to a transmitter of the method of claim 14; therefore it is rejected along similar rationale.

As to dependent claims 42, 43, and 45-47, these claims contain substantially similar subject matter as claims 2, 3, and 5-8; therefore they are rejected along the same rationale.

6. **Claims 9-13, and 28-32,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Medvinsky U.S. Patent Application Publication No. 2002/0094081 (hereinafter '081) in view of

Jung U.S. Patent Application Publication No. 2001/0052072 (hereinafter '072) in further view of Staring U.S. Patent Publication 2001/0007127 (hereinafter '127).

As to dependent claim 9, "further comprising: discarding the data packet if the difference is not less than the threshold value" however '127 teaches "The key check block is sent to the receiver as a header of the current encrypted data payload. The receiver also retains the last eight bytes of the current packet, it decrypted the first eight bytes (the key check block) and compares the result to the retained last eight bytes … If there is no match, an error occurred and the receiver takes appropriate action" on page 5, paragraph 0052.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method key selection for decryption taught in '081 and '072 to include a means to compare the keys being used and take appropriate action (i.e. delete packet) when a match is not found. One of ordinary skill in the art would have been motivated to perform such a modification because of the need to protect data during transmission see '127 (page 1, paragraphs 0005-0006). "It is known to remedy this deficiency by decrypting the data field of the packet with the current session key, as well as the next key in the sequence of keys, and choose the key for which the decrypted data makes sense. Using this method, the change-over from one session key to the next is automatically detected. However, to determine whether the decrypted data makes sense requires knowledge about the information being transmitted. This is not always the case, limiting the use of this method. It is an object of the invention to provide a secure communication system, sink device and secure communication method which overcome above mentioned drawback".

As to dependent claim 10, "further comprising: re-synchronizing a decryption key to an encryption key by setting the decryption key and the encryption key to a start vector if the difference in not less than the threshold value" is taught in '081 page 4, paragraphs 0041- 0053 "it signals the CODEC change to gateway controller 106. MTA 104 generates a new set of RTP key stream and a new initial time stamp. Herein lies a first advantage of the present invention. The related art provides for re-derivation of the RTP key stream when a CODEC change occurs, by providing the following key derivation function … "End-End RTP Key Change <N>" is a label that is used as a parameter to the key derivation function".

As to dependent claim 11, "further comprising: discarding the data packet if the at least a portion of the received message digest value does not match a locally generated message digest value" is taught in '127 page 5, paragraph 0052-0053.

As to dependent claim 12, "further comprising: re-synchronizing the decryption key to an encryption key by setting the decryption key and the encryption key to a start vector if the at least a portion of the received message digest value does not match the locally generated message digest value" is shown in '081 page 4, paragraph 4-5, paragraphs 0054-0057 "In a further embodiment, the above solution is employed for a MAC (Message Authentication Code) algorithm change, resulting in a packet size change. Traditionally, for convenience the same RC4 key stream may be used in the generation of the keying material needed to calculate a MAC for each packet (a MAC is appended after the encrypted text). Where the MAC pad is key used to generate the MAC, for one-time use only. So, wehre a key stream is used for MAC generation (instead of or in addition to encryption) and the size of that

random pad changes, one must rekey and start a new RC4 key stream in the same way as fro CODE changes".

As to dependent claim 13, "further comprising: extracting the at least a portion of the received message digest value from the data packet; generating the locally generated message digest value based on the at least a portion of the received session count, a received encrypted payload of the data packet and a message digest key; truncating the locally generated message digest value to form a truncated message digest; and comparing the truncated message digest to the at least a portion of the received message digest value" is shown in '081 page 4, paragraph 4-5, paragraphs 0054-0057.

As to dependent claims 28-32, these claims contain substantially similar subject matter as claims 9-13; therefore they are rejected along the same rationale.

7. **Claim 57,** is rejected under 35 U.S.C. 103(a) as being unpatentable over Medvinsky U.S. Patent Application Publication No. 2002/0094081 (hereinafter '081) in view of Sengodan et al. U.S. Patent 6,918,034 (hereinafter '034).

As to dependent claim 57, "A receiver comprising: a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold" is taught in '081 pages 3-4 paragraphs 0033-0034;

"a decryption engine configured to decrypt a payload of the received encrypted data packet by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold" is shown in '081 page 2, paragraphs 0017-0018

the following is not explicitly taught in '081: **"a padding engine operable to pad an encrypted payload of the received encrypted data packet to generate the payload of the received encrypted data received by the decryption engine;" "and a pad remover configured to remove padding from the decrypted data"** however '034 teaches that padding is added to packets so that each packet is a predetermined block size in col. 4, lines 30-36.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method encryption/decryption utilizing stream ciphers over the Internet taught in '081 to include a means add padding to the exchanged packets. One of ordinary skill in the art would have been motivated to perform such a modification because there is a need to introduce padding at the packet level see '034 (col. 3, line 65 through col. 4, line 29). "Currently, there exist mechanisms for providing encryption at the IP level and at the RTP level. These mechanisms have taken into account the fact that block encryption schemes require the input to be an integral multiple of the block size. This has been made possible by suitable padding schemes. However, in an environment where several mini-packets are multiplexed into a RTP packet, no suitable encryption (and corresponding padding) mechanism has been proposed … It can be seen then that there is a need to provide padding and encryption on a mini-packet basis. It can also be seen that there is a need for a mechanism to perform padding and encryption at the mini-packet level. It can also be seen then that there is a need for a mechanism to perform authentication at the mini-packet level. To overcome the limitations in the prior art described above, and to overcome other limitations that will become apparent upon reading and understanding the present specification, the present invention discloses a method and apparatus to provide encryption and authentication of a mini-packet in a multiplexed real time protocol (RTP) payload. The present

invention solves the above-described problems by providing a mechanism to perform padding, encryption and authentication at the mini-packet level".

Conclusion

Accordingly, THIS ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

8. It is noted, PATENTS ARE RELEVANT AS PRIOR ART FOR ALL THEY CONTAIN "The use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain." In re Heck, 699 F.2d 1331, 1332-33, 216 USPQ 1038, 1039 (Fed. Cir. 1983) (quoting In re Lemelson, 397 F.2d 1006, 1009, 158 USPQ 275, 277 (CCPA 1968)). A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including nonpreferred embodiments (see MPEP 2123).

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 7:30 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/ELLEN TRAN/

Primary Examiner, Art Unit 2433